UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,807	03/05/2002	Masashi Mitomo	1341.1102CIP	5215

21171 7590 08/21/2007

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
AILES, BENJAMIN A	
ART UNIT	**PAPER NUMBER**
2142	
MAIL DATE	**DELIVERY MODE**
08/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/087,807	MITOMO ET AL.	
	Examiner	Art Unit	
	Benjamin A. Ailes	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,6-34,36 and 38-69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,6-34,36 and 38-69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 14 June 2007 has been entered.

2. Claims 1, 2, 4, 6-34, 36, and 38-69 remain pending.

Response to Amendment

3. Applicant's amendment to claim 65 has been entered into the record and overcomes the prior claim objection. The prior claim objection has been withdrawn.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 68 and 69 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 68 recites the limitation "the external transmission unit" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim. For examination

purposes, it is best understood that "the external transmission unit" refers to the "transmission unit" recited in line 13 of claim 1.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1, 2, 4, 6-19, 26-30, 33, 34, 36, 38-51, 58-62, 65-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard in view of Carter et al. (US 2003/0051026), hereinafter referred to as Carter.

10. Regarding claim 1, Howard discloses a filtering apparatus which is interposed between a client and a server providing a service in accordance with each of access requests from the client, and which transmits only a legal access request among the access requests to the server, the filtering apparatus comprising:

an illegal pattern database which stores patterns of illegal accesses to the server (col. 7, ll. 24-30, Howard discloses the use of a memory location containing one or more patterns that have been defined and make up a pattern collection);

a pattern estimation unit which estimates legality of an access request based on the illegal access patterns stored in the illegal pattern database and on a predetermined pattern estimation rule (col. 7, line 66 – col. 8, line 20, Howard teaches the evaluation of input strings to determine the presence of input strings.);

a pattern determination unit which determines whether each access request is to be transmitted to the server based on the estimation by the pattern estimation unit and on a predetermined pattern determination rule, the pattern determination unit producting a determination result (col. 8, ll. 21-23, Howard teaches that if it is determined that attack patterns are present, then remedial actions are taken as necessary to eliminate risks to the server system).

a transmission unit which controls transmission of the access request based on determination result of the pattern determination unit so as to transmit the access request to the server when the access request is estimated to be legal, and so as to reject transmission of the access request to the server and so as to abandon the request when the access request is estimated to be illegal (col. 7, ll. 36-58, Howard teaches that if no attack patterns have been found, then processing continues as normal and if it is determined that the input string contains attack pattern(s) then remedial action is taken, including the denial of a request altogether from the client to the server.).

Howard does not explicitly teach of wherein the pattern estimation unit calculates a predetermined estimation value according to a degree of correspondence of the access requests to the illegal access patterns stored in the illegal pattern database; and the pattern determination unit compares the estimation value calculated by the pattern estimation unit with a predetermined threshold value, and determines whether the access request is to be transmitted to the server. However, Carter teaches on this aspect in paragraph 0006 and 0447 wherein Carter teaches the calculation of comparisons to prior occurrences to infer appropriate countermeasures and wherein the knowledge learned from new threats may be communicated to other systems. One of ordinary skill in the art at the time of the applicant's invention would have found it obvious to combine what Carter with Howard teaches. One of ordinary skill in the art at the time of invention would have been motivated to make the above mentioned modifications for the reasons discussed in Carter wherein Carter teaches the ability to expand a knowledge base with information relating to unanticipated events is desirable in a network system.

11. Claims 33, 65, 66 and 67 contain similar subject matter and are rejected under the same rationale as independent claim 1.

12. Regarding claim 2, Howard discloses the filtering apparatus wherein

the pattern estimation unit estimates that each of the access requests is an illegal access if the access request corresponds to any one of the illegal access patterns stored in the illegal pattern database, and estimates that the access request is a legal access if the access request does not correspond to any one of the illegal access

patterns stored in the illegal pattern database (col. 8, ll. 21-23, Howard teaches that if it is determined that attack patterns are present, then remedial actions are taken as necessary to eliminate risks to the server system); and

the pattern determination unit determines that the access request estimated as the illegal access by the pattern estimation unit is not to be transmitted to the server, and determines that the access request estimated as the legal access by the pattern estimation unit is to be transmitted to the server (col. 8, ll. 21-23, Howard teaches that if it is determined that attack patterns are present, then remedial actions are taken as necessary to eliminate risks to the server system).

13. Claim 34 contains similar subject matter and is rejected under the same rationale as claim 2.

14. In regards to claim 4 and 36, Howard teaches about a legal pattern database which stores ... and a predetermination unit which predetermines whether each of the access requests corresponds... (col. 7, ll. 36-58). Howard does not explicitly teach of wherein the pattern estimation unit estimates the legality of only the access request determined not to correspond to any one of the legal access patterns by the predetermination unit. Carter teaches on this aspect Paragraph [0006]. One of ordinary skill in the art at the time of invention would have been motivated to make the above mentioned modifications for the reasons discussed in Carter, Paragraph[0005].

15. In regards to Claim 16 and 48 Howard does not explicitly teach of a external transmission unit which transmits each of the access requests determined not to be transmitted to the server by the pattern determination unit, to a predetermined external

device based on a predetermined external transmission rule. Carter implicity teaches on this aspect (Paragraph [0006, lines 17-19). One of ordinary skill in the art at the time of invention would have been motivated to make the above mentioned modifications for the reasons discussed in Carter, Paragraph [0005].

16. In regards to Claim 6,17 and 38, 49 Howard teaches about a storage unit (Fig 4) which stores each of the access request.....(fig. 4).

17. In regards to Claim 7, 18-19 and 39, 50-51 Howard teaches the need for an update unit which updates the illegal pattern database (col. 7, ll. 24-26).

18. In regards to Claim 8, and 40 Howard teaches about an access request transmission unit which transmits, as a legal access request, (col. 7, ll. 36-58) but does not explicitly teach of only the access request determined to be transmitted to the server by the pattern and statistic determination units, to the server statistically illegal request database .... from the statistic of the access requests for the server; a statistic estimation unit ... a statistic determination unit; Carter implicitly teaches on these aspects. Carter teaches of using statistical analysis to detect anomalous events (Page 58, 2nd Col, Claim 20). One of ordinary skill in the art at the time of invention would have been motivated to make the above mentioned modifications for the reasons discussed in Carter, Paragraph [0005].

19. In regards to Claim 9-11 and 41-43 Howard does not explicitly teach of the statistically illegal request database stores transmitting end information on the clients each of which issues access requests.... stores request contents of the access requests....and determines that the access request estimated as the legal access by

the statistic estimation unit is to be transmitted to the server. Carter teaches on these aspects (Page 58, 2nd Col, Claim 20, Paragraph [0205,0204,0216]). Motivation is same as discussed in Claim 8.

20. In regards to claims 12 and 44 Howard does not explicitly teach the statistically illegal request database stores transmitting end information on the clients.... calculates a predetermined estimation value according to a degree to which the transmitting end... Carter teaches on these aspects (Paragraph [0204-0205, 0216,0006]). Motivation is same as discussed in Claim 8.

21. In regards to claims 13-15 and 45-47 Howard teaches about estimating the legality of access request (col. 7, ll. 36-58) but does not explicitly teach of statistic estimation...Carter implicitly teaches on these aspects (Page 58, 2nd Col, Claim 20). It should be noted that Carter is explicit about detecting anomalous; however it would have been obvious to one of ordinary skill in the art at the time of invention to extend his invention so that the statistical analysis can correspond to legal access request as well based on what is taught by Carter in Paragraph [0183]. Motivation is same as discussed in Claim 8.

22. In regards to claims 26-29 and 58-61 Howard does not explicitly teach of an access request decryption step of decrypting... the access request which has been subjected to the predetermined encryption processing. Carter teaches on these aspects (Paragraph [0225-0226]. Motivation is same as discussed in Claim 8.

23. In regards to claims 30 and 62 Howard implicitly teaches of a pseudo-response database which stores pseudo-responses corresponding to the patterns of the illegal accesses to the server...(Figure 4).

24. Regarding 68, Howard and Carter teach the filtering apparatus wherein the external transmission unit selectively edits illegal access information on an access request which is not transmitted to the server by the access request transmission unit (Howard,, col. 7, lines 50-52, remedial actions).

25. Regarding claim 69, Howard and Carter teach the filtering apparatus wherein the illegal access information is selected from the group consisting of: a content of the access request, an address and a host name of a transmitting end of the access request, and a transmission time of the access request (Howard, col. 7, lines 54-58).

26. Claims 31-32 and 63 –64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard as applied to claims 1 and 33 above, and further in view of Carter and Cahill (US 6535855).

27. In regards to claims 31 and 63 Howard does not explicitly teach of decoy unit which receives the access requests each of...Cahill teaches on these aspects (Col 12, lines 50-55, Col 13, lines 20-35). One of ordinary skill in the art at the time of invention would have been motivated to make the above-mentioned modifications for the reasons discussed in Carter (Paragraph [0026]).

28. In regards to claims 32 and 64 Howard implicitly teaches of a pseudo-response database which stores pseudo-responses corresponding to the patterns of the illegal accesses ... and a pseudo-response transmission unit which transmits the pseudo-

responses created by the pseudo-response (Fig. 4). Howard does not explicitly teach of a decoy unit which receives the access requests which do not correspond to the illegal access patterns stored in the pseudo-response database...Carter teaches of access request which do not correspond to the illegal access patterns (Col 9, lines 30-65) and Cahill teaches of a decoy unit (Col 13, lines 20-25). Motivation is the same as discussed in Claims 8 and Claim 17.

29. Claims 20-21 and 52-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard as applied to claim 1 and 33 above, and further in view of Kashani (US 2002/0165894) and Birrel et al. (US 2003/0135555 A1).

30. In regards to Claims 20 – 21 and 52-53 Howard teaches about a database with stores patterns of illegal request (col. 7, ll. 36-58) but does not explicitly teach of illegal responses. Kashani teaches on this aspect (Paragraph [0120]). One of ordinary skill in the art at the time of invention would be motivated to make the above-mentioned modifications for the reasons discussed in an analogous art (Birrel, Paragraph [0004]).

31. Claims 22-25 and 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard as applied to claims 1 and 33 above, and further in view of Carter and Kashani.

32. In regards to claims 22-25 and 54-57 Howard does not explicitly teach about illegal response database..... threshold value....external transmission unit....storage of response that is not transmitted....and update unit.....Carter teaches on threshold value (Paragraph[0006,0218]....external transmission unit(Paragraph[0006]....storage of information that is not transmitted(Paragraph[0006]) that is not transmitted....and

update unit (Paragraph[0253]) but does not explicitly teach about illegal responses. Kashani teaches on this aspect (Paragraph [0120]). Motivation is the same as discussed in Claim 8 and Claim 20.

Response to Arguments

33. Applicant's arguments filed 14 June 2007 have been fully considered but they are not persuasive.

34. Applicants' argue that Howard neither teaches, discloses, nor suggests (A) estimating the "legality of an access request," let alone (B) "a pattern estimation unit which estimates legality of an access request based on the illegal access patterns stored in the illegal pattern database and on a predetermined pattern estimation rule". The examiner respectfully disagrees for the reasons set forth below.

35. (A) Examiner maintains that the Howard reference teaches on the claim limitation of estimating the "legality of an access request" as taught by Howard in column 7, line 66 – column 8, line 20. Howard teaches the evaluation of a string that is being sent from a client to a server location to determine if the string contains an attack pattern. If an attack pattern is found the string can be identified as a string containing an attack pattern and remedial actions may be performed, for example, to block the string from being received at the server. The strings being sent from a client to a server can be for example a regular expression, a URL, or an HTTP verb request. Regarding that to which is claimed by applicants, legality of an access request is best understood given broadest reasonable interpretation, the access request being a message being sent to a server from a client device wherein legality of the message is understood as the

determination of whether or not a message should or should not be allowed to be forwarded to a server. This interpretation is based on what is provided in the applicants' filed specification for example on page 13, lines 13-20. No real guidance is given within the claims as to what extent the term "estimation" is to be interpreted regarding scope. Therefore, what Howard teaches is deemed to be within the scope of the claimed limitation.

36. (B) Examiner maintains that the Howard reference teaches on the claim limitation of "a pattern estimation unit which estimates legality of an access request based on the illegal access patterns stored in the illegal pattern database and on a predetermined pattern estimation rule". Howard teaches in column 7, line 66 – column 9, line 20 the evaluation of input strings to determine the presence of input strings. Howard teaches in column 7, lines 24-30 the use of memory that contains one or more patterns that have been defined and make up a pattern collection. Therefore, in view of point (A) and what is further taught by Howard, Howard does teach on the claim limitation "a pattern estimation unit which estimates legality of an access request based on the illegal access patterns stored in the illegal pattern database and on a predetermined pattern estimation rule".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin A. Ailes whose telephone number is (571)272-3899. The examiner can normally be reached on Monday-Thursday 6AM-10PM in accordance with IFP.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

baa

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER